Educational Administration: Theory and Practice
2023, 29(4), 2350-2353
ISSN: 2148-2403
https://kuey.net/

Research Article

Rise In Cyber Crimes Vis-À-Vis Phishing During Pandemic

Mr.Santosh S. Pawar[1*], Dr. Padmaja D. Khatikar[2]

[1] *BE (MECH), BA (ECO), MOM, LLB, LLM, MSW, MCA. Research Scholar, Faculty of Law, Departmet of Law & Governance, Vishwakarma University,Pune.
[2]LLB, LLM, Ph.D, Assistant Professor and Research Guide Cum Co-Author, Faculty of Law, Department of Law & Governance, Vishwakarma University,Pune.

Citation: Mr.Santosh S. Pawar et al (2023), Rise In Cyber Crimes Vis-À-Vis Phishing During Pandemic, *Educational Administration: Theory and Practice*, 29*(4)* 2350-2353
Doi: 10.53555/kuey.v29i4.7105

ARTICLE INFO

ABSTRACT

The world largely faceed the threat of Covid-19. It has hampered the world at large in terms of physical health as well as the economy has also been hit. As a preventive measure lockdown has been enforced to maintain social distancing and to ensure that the virus doesn't spread by contact. Due to this stigma "Work from Home" is what the organizations had to enforce. Not only economy but educational institutions are also resorting to online mode. As we all know there's always a dark side to a coin, so also this online stream is. Now a day's all our transactions are linked with our mobile phones/tabs and other devices, it's just a matter of click and our work is done. So much sensitive information we carry in our devices. This paper critically analyzes cons of online streaming and specifically phishing attacks.

KEYWORDS: Phishing, Cyber Law, Cyber Security, Covid-19, Online Scams

1. INTRODUCTION

Phishing is a cybercrime in which a target or targets are approached by email, telephone or text message by someone acting as a reputable organisation to entice victims into supplying sensitive data such as personally identifying information, banking and credit card details, and passwords. The information is then utilised to access critical accounts and can result in identity theft and financial loss. The first phishing case was brought in 2004 against a Californian teenager who established the replica of the website "America Online". With this phoney website, he was able to acquire sensitive information from customers and access the credit card data to withdraw money from their accounts. More than email and website phishing, there's also 'vishing' (voice phishing), 'smishing' (SMS Phishing) and numerous other phishing tactics hackers are continuously coming up with. Crime is timeless. It is in the society since beginning and will be there forever. With changes in the society, the approaches of criminals will be changing**.** Similarly the approach to combat such crime keeps changing by different depending upon the nature and extent of the crime.

SELECTION OF RESEARCH TOPIC WITH REASONING

Technology and crime today are going hand at hand. The event in technology is additionally giving rise to crimes wherever this technology is employed or say abused. All our data and different transactions are on our finger tips. Each single day we tend to open a newspaper we do bump into cyber crimes whereby individuals are being duped of with a lot of cash and amazingly they solely dole out the knowledge. In phishing the phisher masquerades himself to be the real or legitimate person whereby the victim beneath being impression that he's revealing information to the real person shells out his data and falls prey to such act of phishing. for example, you're obtaining associate email from your bank for change your personal data or such kind. You are doing it beneath a sway that it's from your bank whereas it's from the phisher in order that he will use your data to commit his crime. The provisions of the IT Act are elicited for the aim of addressing phishing as like of the other cyber crime. There is clearly a necessity felt to own associate exclusive Act or provision for phishing that is additionally recognized by the Indian courts. The reasoning of selection of proposed research topic is logical as it will help the members of bar and bench to understand effect of such provision which will exclusively deal with Phishing.

IMPORTANCE OF RESEARCH

In India, numerous cases of phishing are noted chop-chop since 2004 close to. In India there's no special legislation that deals with phishing. It's obscurity outlined in Indian legislation. It comes under the provisions of the Information Technology Act, 2000. The IT Act protects and acknowledges numerous digital transactions and deals with penalization just in case of infringement of any provisions. It requires in-depth research to make law effective and efficient to prohibit it. The research will be very useful for the lawyers and also to the Courts in deciding the complex cases relating to Cyber crime "Phishing". This research is a sincere attempt to explore the complex cyber crimes which may enable a better understanding of the issues involved.

2. COMMON FEATURES OF PHISHING

a. Too Good To Be True - Lucrative offerings and eye-catching or attentive remarks are meant to instantly draw the attention of individuals. For example, many say you won an iPhone, a lottery or some other award. Just don't click any emails you suspect. Remember, it usually is, if it appears good to be true!
b. Urgency sense - One of hackers' favourite tactics is to suggest that you act quickly since the amazing offers are for a limited period. Some of them will even say you just have a few minutes to answer. When you find e-mails of this sort, it is better to disregard them. Sometimes, you are told that your account is suspended until you quickly update your personal data. Most trustworthy businesses provide enough time before they end an account and never require employers to update personal data on the Internet. In case of uncertainty, visit the source directly instead of clicking on the link in an email.
c. Hyperlinks - A link may not be what it seems to be. If you hover over a link, you will see the current URL where you are directed when you click it. It may be totally different or a popular site with mispellings, such as www.bankofarnerica.com - the 'm' is a 'r' and a 'n' actually, so look at it carefully.
d. Annexes - If you notice an annex in an email or if this does not make sense, don't open it! Do not open it! Often they include payloads such as ransomware or other infections. The only file type you can always click on is a.txt file.
e. Unusual Sender – Whether it seems to be someone you don't know about or someone you know, if anything seems out of the ordinary, surprising, uncharacteristic or generally simply suspicious, don't click it!

3. RISE OF PHISHING CASES DURING PANDEMIC

What started from the city of Wuhan, China has taken a massive toll on human life all over the world. No one had ever imagined the world will witness this kind of pandemic, where the world stood still. All the trade, IT sector and other professions got majorly hit by the situation. To sustain this phase we all had to resort to taking up the work online whereby by staying at their respective place people opted to work instead of going to the offices or institutes (Work from Home). The education institutions too are working online the real classrooms are now virtual or digital classrooms. As the number of the use of internet or cyber is on the massive rise so does the threats that are posed by it. It is an abundance trap for the cyber attackers.
The International Criminal Police Organization has launched a campaign to raise awareness of cyber-related threats throughout the COVID-19 explosion. The campaign runs from 4 to 31 May 20.
Cooperation with law enforcement authorities has been developed across the globe. A multinational network delivered easy tips on cyber hygiene. This will ensure that individuals and companies are well prepared to monitor their processes and records.
Cyber criminals take advantage of the concerns caused by COVID-19. They use techniques such as data mining ransomware, malware, email scams and phishing scams. According to a website, Hackers used the coronavirus confusion to make individuals give up personal data and sensitive information and cash.
Hundreds of thousands of emails from Covid-19 are sent regularly, and some computer security experts say that in years or ever the virus has been the most relevant target for scams from phishing.
This website gathers them and classifies them according to attributes. It has collectively logged any keywords or sentences that can be scanned for if your email is on the list of phishing scams.
Malicious emails that could raise you to open an attachment which supposedly contains relevant information concerning the region of Coronavirus, unit that can pass malicious code on your computer as long as you press the attachment or embedded connection. This code will allow cyber criminals to manage your device, record your keystrokes or access your personal details and currency information, which can lead to theft.
In addition, there is a rapid growth in identity fraud initiatives, and also in typing websites – domain names which can be viewed as branded brands for internet stores or used to steal personal details from criminal campaigns. Apparently, the main priority for this movement is the high-end retail unit.
For example, from 1 March to 30 April 2020, Future Record reported 163 registered domains or domains registered for Amazon affiliation. Many malicious domains are meant as fake websites, such as mail[..] amazon-login[.] online, with the intention of including a different local agency in phishing emails to steal such confidential information, such as amazon payments[..] theworkpc[.] com. After all, Amazon is n aim at the same time – more relevant marketing corporations have seen domain registration grow aimed at all.

Microsoft announced on 14 May that it had a new package to provide free IOC/COVID-19 feeds. These functions are physically incorporated into most Microsoft security technologies. Multi-vendor sites are nevertheless prepared to use IOCs if required. Hash-based IOCs provide numerous files and hazard forms, and sell the Microsoft Graph Protection API easily and Azure GitHub protection. MISP company harassment can just send/add additional details.
Spam/phish authenticity gathering campaigns and COVID topicware for mechanical man highlights for the update this week. Attackers use several novels to steal classified information in their terrorist campaigns and even to change some of the more common ones (e.g. FedEx and UPS criminal identity theft traps).
1.755 warnings were issued to identity fraud customers by the Google Threat Analytical Cluster, a Threat Detection Cluster diary, recorded payments. Alert suggests that attempts to hack and steal sensitive data are increasing, as stated by Google above, by harassing cyber criminals who use the coronavirus as a basis of their tactics. The diary lists corporations, forums of consultation, and health services in most of the high-risk regions.
Maor noted that there are a variety of ways people should defend themselves from being unknown cyber criminals.
Second, they should be aware of the probability of these threats. "Attackers are involved in those threats, work in technologies, systems and individuals. You see these flaws, you work hard to find them. People therefore ought to see that they are the victims of such attacks, "He said. He said.
Next, keeping safety transparent is important: in addition to the misuse of advanced security mechanisms such as two-factor authentication or VPNs, it also updates the kit to keep it up to date. While they are not unreasonable, they prohibit people from being straight blocks.
"When you politely suspect your email appearance, don't open it. Or click either of the links. When they appear as the bank or currency advisors, determine and lift them."

4. PHISHING - A CYBER CRIME, THE PROVISIONS OF INFORMATION TECHNOLOGY ACT, 2000

The phishing fraud essentially is a cybercrime and it attracts many penal provisions of the Information Technology Act, 2000 as amended in 2008 adding some new provisions to deal with the phishing activity. The following Sections of the Information Technology Act, 2000 are applicable to the Phishing Activity:
Section 66: The account of the victim is compromised by the phisher which is not possible unless & until the fraudster fraudulently effects some changes by way of deletion or alteration of information/data electronically in the account of the victim residing in the bank server. Thus, this act is squarely covered and punishable u/s 66 IT Act.
Section 66A: The disguised email containing the fake link of the bank or organization is used to deceive or to mislead the recipient about the origin of such email and thus, it clearly attracts the provisions of Section 66A IT Act, 2000.
Section 66C: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say Logo, trademark etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000.
Section 66D: The fraudsters through the use of the phishing email containing the link to the fake website of the bank or organizations personates the Bank or financial institutions to cheat upon the innocent persons, thus the offence under Section 66D too is attracted.
The Information Technology Act, 2000 makes penal provisions under the Chapter XI of the Act and further, Section 81 of the IT Act, 2000 contains a non obstante clause, i.e. “the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force”. The said non obstante clause gives an overriding effect to the provisions of the IT Act over the other Acts including the Indian Penal Code. The aforesaid penal provisions of the IT Act, 2000 which is attracted to the phishing scam are however been made bailable by virtue of Section 77B IT Act intentionally in view of the fact that there is always an identity conflict as to the correct or accurate identity of the person behind the alleged phishing scam and there is always a smokescreen behind the alleged crime as to the identity of the person who has actually via these online computer resources have or have not committed the offence and in view of the possible misuse of the penal provision for cyber offences as contained in the IT Act, the offence is made bailable.

5. WAYS TO PROTECT FROM SCAMS AND CORONAVIRUS SCAMS:

1) Do not respond to calls or messages from unknown or suspected numbers.
2) Never email, text message or phone to share your personal or financial information.
3) Be vigilant anytime you have to exchange some data or now make a bill.
4) Scammers often give telephone numbers for answering or replying. Note that government officials cannot determine if personal details or money are to be welcomed.
5) Do not click any text message links. If a fan sends you a text with a suspicious connection that seems absent from the character, you plan to do something not hacked.

6) Before offering, often look at the platform (e.g. by company or by looking at the own website).[1]

6. PREVENTING PHISHING ATTACKS:

Although hackers are continuously developing new tactics, you may do certain things to protect yourself and your organisation:

a. Spam filters can be used to guard against spam email. The filters generally analyse the communication's origin, the software used to deliver the message and the message appearance in order to identify whether it is spam. Sometimes, spam filters might even prevent email from reputable sources, so that it is not always 100% correct.

b. The browser settings should be adjusted to avoid the opening of fake websites. The browsers retain a record of the phoney sites and the address is banned when you try to visit the site or an alert message is displayed. The browser settings should only open reputable websites.

c. Many websites ask visitors to submit login information while displaying the user picture. Such a system can be vulnerable to security threats. One method to maintain security is by regularly changing passwords and never using the same password for numerous accounts. It is also a good idea for websites to utilise an extra security CAPTCHA system.

d. Banks and financial institutions employ phishing prevention monitoring systems. Individuals can report phishing to business groups where legal action against such fake websites might be initiated. Organizations should offer staff with safety awareness training to detect dangers.

e. To prevent phishing, changes in surfing behaviour are necessary. If verification is necessary, always call the firm before providing any online data.

f. If you have a link in an email, first float over the URL. Secure websites with a valid SSL certificate begin with "https." "https" All sites will eventually have to have a valid SSL.

g. Additionally, while using any monetary or banking app make sure to turn off the data from the settings and to on it only when you are to do any transaction. The passwords always should contain combination of numeric and symbol with alphabets. Updating passwords periodically again is very important.

CONCLUSION

As it has been said that prevention is better than cure, we must all have to be more vigilant and aware about the cons of using internet. Ignorance here would land one in the trap of cyber attack. As in the case in country like India though the lockdown is been relaxed but to the contrary the virus is on rise ever than before. We have to live with this state. It is unpredictable whether when everything will be normal what all we can do is to sustain with the current situation and be cautious. Internet is serving as a blessing to us; a great tool because of which the work can be done from any part of the world which is proved with this pandemic. We must vigilant at all times let it be Pendamic or Normal situation such attakers and attacks are always on rise so we have to face these situations with all available majors and tools to conter such attakers and attacks with every possible means.

REFERENCES

1. Dongre Shilpa S.(2010) -Cyber Law and its implementations.
2. Dr. Vishwanath Paranjape. (2010)-Legal Cyber and Preventive Law DimensionP.-14.
3. Guidelines on Electronic Mail Security Recommendations of the National Institute of Standards and Technology Special Publication 800-45 Version 2.
4. https://coronavirusphishing.com/(last visited on 21st June2021).
5. https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic (last visited on 8th July 2021).
6. https://www.fcc.gov/covid-scams last visited on 20th June 2021
7. https://www.fcc.gov/covid-scams last visited on 20th June 2021
8. https://www.metacompliance.com/resources/ultimate-guide-to-phishing/(last visited on 28/6/2021)
9. https://www.recordedfuture.com/pandemic-retail-phishing-campaigns/ (last visited on 8th July 2021)
10. https://www.thehindu.com/news/international/cyberthreats-during-the-covid-19-pandemic/article31572810.ece (last visited on 20th June 2021).

[1] https://www.fcc.gov/covid-scams last visited on 20 th June 2023